明 細 書

電子データ管理装置、その制御プログラム及び電子データ管理方法

技術分野

[0001] 本発明は、ユーザのデータを格納し、管理する電子データ管理装置、その制御プログラム、及びデータ管理方法に関する。詳しくは、電子計算機に接続して使用する電子データ管理装置、その制御プログラム、及びデータ管理方法に関する。更に詳しくは、生体情報、暗証番号、鍵等を利用して個人認証を行い、メモリに格納されているデータへのアクセスを許可する電子データ管理装置、その制御プログラム、及びデータ管理方法に関する。

背景技術

[0002] 電子計算機にアクセスするときに、ユーザの認証を行っている。このユーザ認証には、ユーザ名とパスワードをキーボードから入力するパスワード式認証、人間の指紋、掌形、声紋、顔、虹彩等の生体情報を利用するバイオメトリクス認証がある。また、電子計算機と接続して利用する周辺装置を使用するときもユーザ認証を行うことができる。

[0003] 特に、外部記憶デバイスへアクセスするとき、セキュリティ面からは、ユーザ認証が重要である。従来から、電子計算機の本体、その周辺装置の電源、ケースなどに暗証番号又は鍵付きのロックを設けているものがある。その暗証番号を知っているユーザ又はその鍵を所持しているユーザのみが電子計算機を利用することができる。

[0004] 外部記憶デバイスとして利用されている記憶メディアとしては、数多くの種類がある。代表的なものとしては、ハードディスク、MO、DVD−RAMがある。これらの記憶メディアはギガバイト以上の大容量のメディアである。近年、記憶メディアとしてのフラッシュメモリが数多く開発されて著しい普及を遂げている。コンパクトフラッシュ（登録商標）、スマートメディア（登録商標）、メモリスティック（登録商標）等のフラッシュメモリは、数十から数ギガバイト容量の記憶メディアである。

[0005] ユーザはこれらの外部記憶メディアにデータを記録して別の場所で再生したり、作業を継続したりする他、必要に応じて他人にデータを渡すときにも利用している。これ

らの外部記憶メディアの記録データを再生、記録するデバイスが、USB(Universal Serial Bus)等のインターフェースで電子計算機に接続されて、記録データの送受信を行っている。

[0006] 例えば、マイクロソフト社(登録商標)の Windows Me(登録商標)、 Windows 2000(登録商標)、 Windows XP(登録商標)等のOS(Operating System)の場合は、PnP(Plug and Play)機能を利用して電子計算機に接続されたデバイスを自動認識している。上述の外部記憶メディアの記録データを再生、記録するデバイスも同様にPnP機能を利用してOSに自動認識されている。

[0007] USBインターフェースで電子計算機にデバイスを接続すると、OSのPnP機能が自動的にデバイスを認識して必要なドライバをインストールするか、又はドライバインストールの指示を画面に表示させて、ユーザはその指示に従ってドライバをインストールして、接続デバイスを利用できる環境を電子計算機上に提供している。これにより、接続された外部記憶デバイスの記録データを読み込んだり、外部記憶デバイスへデータを書き込んだりする。

[0008] 電子計算機を利用しようとするとき、記憶メディアに生体情報の一つである指紋認証情報を設けている例がある。例えば、特許文献1の「可搬性記録媒体及び可搬性記録媒体の使用方法」においては、CD-RWにアプリケーションソフトウェア、ユーザ認証プログラム、指紋認証エンジンと、利用者の指紋情報等を格納して、指紋照合によるユーザ認証、認証後のアプリケーションソフトウェアの利用を提供している。

特許文献1:米国公開特許番号 US2001014883 A1-2001-08-16、"Portable recording medium and method of using portable recording medium".

発明の開示

発明が解決しようとする課題

[0009] フラッシュメモリ等にユーザデータを記録して運び、別の電子計算機でそれを読み込んで使用する場合、又は他人に渡して利用してもらう場合がある。しかし、ユーザにとっては、一般的にユーザデータは重要なものであり、これらのユーザデータをそのまま第三者に渡すことは元より、電子計算機にも残したくない。例えば、印刷業者に頼んでそのデータの文字、写真等の情報を印刷するとき、ユーザは印刷データを

フレキシブルディスクやCD−ROMなどの媒体に入れて提供することが一般的である。印刷業者がこれらの印刷データを利用して印刷した後は、媒体を発注元に戻しても、印刷データが業者の電子計算機内に残ることになる。これはユーザにとってセキュリティの面では好ましくない。

[0010] 本発明は上述のような技術背景のもとになされたものであり、下記の目的を達成する。

本発明の目的は、電子計算機と接続されると自動的にインストールされて利用されるもので、電子計算機内のデータの制御を行うことができる制御プログラムを格納した電子データ管理装置、その制御プログラム、及び電子データ管理方法を提供する。

本発明の他の目的は、電子計算機から切断されると電子計算機に送信された、または電子計算機内に加工されたデータ、作成されたファイル等を消去することができる制御プログラムを格納した電子データ管理装置、その制御プログラム、及び電子データ管理方法を提供する。

[0011] 本発明の更に他の目的は、電子計算機から切断されると自ら消滅する又は無効になることができる制御プログラムを格納した電子データ管理装置、その制御プログラム、及び電子データ管理方法を提供する。

本発明の更に他の目的は、個人認証機能を有する電子データ管理装置、その制御プログラム、及び電子データ管理方法を提供する。

課題を解決するための手段

[0012] 本発明は、前記目的を達成するため、次の手段を採る。

本発明の第1の発明の電子データ管理装置(1、20、30)は、データを記憶するデータ記憶手段(6)と、認証用の識別データが登録されている識別データ記憶手段(11)と、ユーザの認証情報を入力する入力手段(3、21、31、32)と、前記入力手段(3、21、31、32)からの入力データと、前記識別データ記憶手段(11)に登録された前記識別データとを比較して前記ユーザの認証を行う認証手段(12)と、電子計算機と接続して前記データの送受信を行うインターフェース手段(9)と制御プログラムを記憶するプログラム記憶手段(7)を有する。

[0013] 前記電子データ管理装置(1、20、30)は、前記認証の結果、前記入力データと前記識別データが一致するときに前記データへのアクセスを許可し、前記認証手段(12)によって前記ユーザが認証された後、前記制御プログラムが前記電子計算機にインストールされ、前記電子計算機から前記データを読み出しすることが可能になると良い。

[0014] また、前記認証手段(12)による前記認証が完了した後、前記電子データ管理装置(1、20, 30)のロックが解除されて、接続されている前記電子計算機が前記電子データ管理装置(1、20, 30)の自動認識を開始すると良い。

更に、前記データ記憶手段(6)と前記プログラム記憶手段(7)とをスイッチするスイッチ制御手段(10)を有すると良い。

[0015] 更に、前記電子計算機から前記データ記憶手段(6)に書き込みすることが可能で、前記データを用いて前記電子計算機で操作した履歴又は前記電子計算機を操作した履歴が書き込まれると良い。前記識別データは指紋データで、前記入力手段(3)から前記ユーザの指紋情報を入力し、前記認証手段(12)により前記ユーザの指紋認証を行うと良い。

[0016] 更に、前記識別データは登録暗証番号で、前記入力手段(21)から暗証番号を入力し、前記認証手段(12)により前記暗証番号と前記登録暗証番号とを比較して前記ユーザの認証を行うと良い。更に、前記認証手段(12)は錠(32)と鍵(31)を有し、前記鍵(31)を持っている前記ユーザに前記データへのアクセスを許可すると良い。

[0017] 本発明の第2の発明の電子データ管理装置用制御プログラムは、電子データ管理装置(1、20、30)内に記録されている制御プログラムであり、電子データ管理装置(1、20、30)は、制御プログラムを記憶するプログラム記憶領域(7)を有し、前記認証が行われた後に前記制御プログラムが電子計算機にインストールされ、前記電子計算機で前記データを利用して作業を行うとき、前記作業の履歴を記憶するように前記電子計算機を動作させるプログラムである。

[0018] また、前記電子データ管理装置(1、20、30)は、登録された認証用情報を記憶する認証用情報領域(11)と、ユーザの識別情報を入力する入力部(3、21、31、32)と、前記認証用情報と、前記識別情報とを比較して前記ユーザの認証を行う認証機能

を有する認証部(12)と、データを記憶するデータ記憶領域(6)とを有し、前記電子計算機と接続されると前記認証部(12)によって前記ユーザの前記認証を行い、前記認証が完了すると、前記ユーザには前記データ記憶領域(6)にアクセスする許可を与えると良い。

[0019] 更に、前記電子データ管理装置用制御プログラムは、前記電子計算機との前記接続が切断されるとき、前記制御プログラムが前記電子計算機内に送信された前記データを削除すると良い。更に、前記制御プログラムが、前記電子計算機と前記電子データ管理装置(1、20、30)との前記接続が切断されると、前記制御プログラムに内蔵された消滅機能を備えた自動消滅プログラムにより自動消滅する機能を有すると良い。更にまた、前記制御プログラムは、前記電子計算機内で動作をしない状態、つまり無効になる機能を有すると良い。

[0020] 更に、前記制御プログラムは、前記電子計算機で前記データを、複製、削除、編集、閲覧、読込み、及び書込み、から選択される一以上の履歴、又は前記データを用いて作成したファイル若しくは新規データの履歴を取得する履歴取得機能と、前記履歴を前記データ記憶領域(6)に書き込みするデータ記録機能と、通信手段を利用して前記履歴を別の電子計算機に送信する送信機能とを有すると良い。

[0021] 更に、前記履歴は、前記電子計算機の入力手段から操作した操作履歴であると良い。前記履歴は、前記電子計算機のキーボードから入力された入力履歴、又はマウスを操作した操作履歴であると良い。更に、前記制御プログラムが前記データを前記電子計算機内に特定アプリケーションで、又は任意に複製、削除、編集、閲覧、読込み、及び書込み、する操作のいずれか一以上の操作だけをできるように前記電子計算機のファイルシステムに制限をすると良い。電子データ管理装置用制御プログラムが、前記電子計算機のOSの全命令を実行できるカーネルモードで動作すると良い。

[0022] 本発明の第3の発明のデータ管理方法は、認証用情報を記憶する認証情報記憶部(11)と、ユーザの認証情報を入力する入力部(3、21、31、32)と、前記入力部(3、21、31、32)からのデータを用いて前記ユーザの認証を行う認証部(12)と、データを記憶するデータ記憶部(6)とを有する電子データ管理装置(1、20、30)が電子計算機に接続され、前記認証部(12)によって前記ユーザの前記認証が行われ、前

記認証情報記憶部(11)に登録された前記認証用情報と一致する前記認証情報を有する前記ユーザに前記データへのアクセスを許可するデータ管理方法であって、前記電子データ管理装置(1、20、30)が制御プログラムを格納するプログラム記憶部(7)を有し、前記認証が終わると前記制御プログラムが前記電子計算機にインストールされ、前記電子計算機で前記データを利用する利用環境を確保する。

[0023] また、前記利用環境は、前記電子計算機で動作する特定アプリケーションプログラムからのみ前記データへアクセスすることを許可する制限であると良い。

更に、前記制御プログラムは、前記電子計算機の入力手段を操作した操作履歴、又は前記データを用いて複製、削除、編集、閲覧、読込み、及び書込み、する操作から選択される一以上の前記データへのアクセスの履歴、又は前記データを用いて作成したファイル若しくは新規データの履歴を残す機能を有すると良い。

[0024] 更に、前記電子データ管理装置(1、20、30)と前記電子計算機との前記接続が切断されると、前記制御プログラムは、前記電子計算機内の前記データ、前記データの複製、前記データを利用して作成したデータ又はファイルの内の1つ以上を削除すると良い。更に、前記制御プログラムが自動消滅する機能を有すると良い。更に、前記制御プログラムは、前記電子計算機内で活動をしない状態、つまり無効になる機能を有すると良い。

発明の効果

[0025] 本発明によると、次の効果が奏される。

本発明は、制御プログラムを格納した電子データ管理装置を提供することによって、制御プログラムは電子データ管理装置が接続されている電子計算機にインストールされ、電子計算機上にユーザデータを用いて行う作業を監視し、電子計算機上に動作するアプリケーションプログラムを制御するためユーザが意図しないことにユーザデータを利用できないようにする。

[0026] また、本発明は、電子計算機でユーザデータを利用した作業後、ユーザデータ、ユーザデータを利用して作成されたファイルの削除を行うことができる制御プログラムを格納した電子データ管理装置を提供している。よって、ユーザデータの漏洩防止等のセキュリティを向上させることが可能になった。更に、個人認証機能を有する電子

データ管理装置を提供することによって、ユーザデータは正当な利用のみに限定し、セキュリティを向上させることが可能になった。

発明を実施するための最良の形態

[0027] 以下、本発明の最良の実施の形態を図面によって具体的に説明する。

〔実施の形態1〕

以下、本発明の実施の形態1のシステムを図面に従って説明する。図1には、本発明の実施の形態1の電子データ管理装置1の外観を示す外観図である。ユーザは、ユーザのデータ及びファイル等のユーザデータを持ち運びするためにこの電子データ管理装置1を使用する。ユーザは、電子計算機にこの電子データ管理装置1を接続して、電子計算機上に動作しているアプリケーションプログラムから電子データ管理装置1に格納されているユーザデータを読み出して作業を行う。

[0028] ユーザは、ある電子計算機に格納されているユーザデータを電子データ管理装置1に記録して持ち運び、別の電子計算機で使用するときにこの電子データ管理装置1を利用しても良い。また、管理者は、ある電子計算機に格納されているユーザデータを電子データ管理装置1に記録し、作業者にこの電子データ管理装置1を渡し、作業者は別の電子計算機でこの電子データ管理装置1を接続してユーザデータを使用するときに利用しても良い。

[0029] 電子データ管理装置1には主に2種類のデータが格納されて保存されている。1つは、上述のユーザデータで、もう一方は制御プログラムである。制御プログラムは、電子データ管理装置1が接続された電子計算機にインストールされて、この電子計算機でユーザデータを用いて作業できる環境を提供するためのプログラムである。制御プログラムは、電子計算機にインストールされると、電子計算機上に動作しているOSの動作、アプリケーションプログラムを監視する。

[0030] 特に、アプリケーションプログラムが電子データ管理装置1に格納されているユーザデータを呼び出して使用するとき、制御プログラムがこのアプリケーションプログラムの動作を監視し、その動作の履歴、ユーザデータの利用、ユーザデータを利用して作成されたファイル等の履歴を取得し電子計算機に保存する機能を有する。また、制御プログラムはこの保存された履歴を電子データ管理装置1に、または通信回線

を介して別の電子計算機に送信する機能を有する。

[0031] ユーザは、これらの機能によって、電子データ管理装置1に格納されているユーザデータの利用状況を把握することが可能になる。制御プログラムは、電子計算機上に動作しているOSの動作、アプリケーションプログラムの機能を制限又は制御する機能を有する。これによって、制御プログラムは、電子データ管理装置1に格納されているユーザデータの利用状況をユーザが意図しないことに利用できないようにする。

[0032] また、電子計算機にインストールされた制御プログラムが自動消滅する機能を有し、電子計算機での作業が完了したら制御プログラムが自動消滅し、電子計算機に残らない。このように本発明の実施の形態1は、電子データ管理装置1と、電子データ管理装置1に格納された制御プログラムを提供している。制御プログラムは、電子データ管理装置1が接続されている電子計算機にインストールされて、この電子計算機においてユーザデータを使用する状況を把握することができるシステムを本発明の実施の形態1が提供している。

[0033] 電子データ管理装置1の構造、電子データ管理装置1の構成部分の動作、制御プログラムの動作、及び電子データ管理装置1と制御プログラムからなる電子データ管理用のシステムの動作および利用について下記に詳しくは説明する。電子データ管理装置1は、筐体2、筐体2の一面に設けた指紋情報入力部3、筐体2と接続されているコネクタ4から構成されている。図2には、筐体2に格納されている基板5の構成の概要を図示している。

[0034] 基板5の上には、第1メモリ6、第2メモリ7、USB(Universal Serial Bus)コントローラ9、中央演算装置(CPU、Central Processing Unit)8等が搭載されて配置されている。第1メモリ6は、ユーザのデータ及びファイル等のユーザデータを格納するためのメモリである。第2メモリ7は、制御プログラム(説明は後述する。)を格納するためのメモリである。USBコントローラ9は、コネクタ4を介して電子計算機(図示せず)との送受信を制御するためのプログラムである。CPU8は、電子データ管理装置1全体を制御するための中央演算処理装置である。指紋情報入力部3及びその指紋情報の認識方法等の技術については、周知の技術であり、かつ本発明の要旨でもないので、その詳細な説明は省略する。

[0035] ユーザデータと、制御プログラムは電子データ管理装置1の別々のメモリ領域である第1メモリ6と第2メモリ7に格納されている。この2つのメモリ領域は、電子計算機から同時にアクセスできないような設計になっている。スイッチ10は、CPUによってソフトウェア的に制御されるもので、電子計算機から第1メモリ6と第2メモリ7へのアクセスを制御するためのものである。

[0036] 電子データ管理装置1が電子計算機と接続され、制御プログラムが電子計算機にインストールされると、スイッチ10が第2メモリ7から第1メモリ6へと切り替わり、ユーザデータの送受信が可能になる。また、基板5には、認証用データベース11、認証モジュール12が配置されている。認証モジュール12は、指紋情報入力部3と連動してユーザの認証を行うためのものである。認証用データベース11は、電子データ管理装置1を使用できるユーザの指紋情報等の識別データを格納したデータベースのためのメモリである。

[0037] 図3は、電子データ管理装置1へこの識別データを記録する手順を示すフローチャートである。図3に図示したように、電子データ管理装置1を利用する前に、ユーザ又は管理者が専用のアプリケーションプログラムによって電子データ管理装置1にユーザデータを書き込み、ユーザの指紋情報が登録される。ユーザ又は管理者は、電子データ管理装置1へユーザデータを書き込みするための専用のアプリケーションプログラムがインストールされている電子計算機に、電子データ管理装置1を接続して、その専用のアプリケーションプログラムによってユーザデータを電子データ管理装置1の第1メモリ6に書き込む(ステップ1)。

[0038] そして、ユーザ又は管理者は、電子データ管理装置1を利用するユーザの指紋情報などの識別データを認証用データベース11に登録する(ステップ2)。識別データの登録が完了すると、ユーザ又は管理者は、電子計算機から電子データ管理装置1を抜き取って持ち出しが可能になる(ステップ3)。これらのユーザデータ及び、ユーザの指紋情報などの識別データは、専用のファイルシステムを用いて行われても良い。

[0039] 図4は、電子データ管理装置1を利用するときの全体の流れを図示したフローチャートである。ユーザ又は作業者は、電子データ管理装置1を電子計算機にUSBコネ

クタを用いて接続する(ステップ10)。電子データ管理装置1はすぐには使用することができない。電子データ管理装置1がロックされていて、電子計算機に接続されても電子計算機から認識することも、電子データ管理装置1にアクセスすることもできない。電子データ管理装置1を利用するユーザ又は作業者は、電子データ管理装置1内に格納されているユーザデータを利用するためには、個人認証(ユーザ認証)を行うことが必要である。

[0040] 個人認証(ユーザ認証)は、ユーザ又は作業者が指紋情報を指紋情報入力部3から入力して指紋認証によって行われる。この個人認証が成功すると、ロックが解除される。そのために、ユーザ又は作業者は、指紋情報入力部3に指を当てて指紋認証を行う。言い換えると、電子データ管理装置1がユーザの指紋認証を行う(ステップ11)。ユーザの指紋認証は、指紋情報入力部3からの指紋情報データを用いて認証モジュール12が行う。

[0041] このとき、認証モジュール12はユーザの指紋情報データを予め登録した識別データと比較して、「正当なユーザであるか？」を判定する(ステップ12)。ユーザの指紋情報データが認証用データベース11に格納されている識別データと一致しない場合は、認証モジュール12は「利用許可がないユーザ」と判定し、ユーザ又は作業者は電子データ管理装置1を利用することができない(ステップ13)。

[0042] ユーザの指紋情報データが認証用データベース11に格納されているデータと一致する場合は、認証モジュール12は「正当なユーザである」と判定し、次の処理に移る。認証モジュール12は電子データ管理装置1のロックを解除し、OSのPnP機能がUSBコネクタ4によって接続されている電子データ管理装置1を、自動認識する処理が許可されPnP機能が開始する(ステップ14)。PnP機能によって電子データ管理装置1をOSが認識し、電子計算機と電子データ管理装置1との間にデータの送受信を行うことが可能になる。初期設定では、電子計算機は第2メモリ7と通信できるように、スイッチ10が設定されている。そして、第2メモリ7に格納されている制御プログラムが、電子計算機にインストールされる(ステップ15)。制御プログラムは電子計算機にインストールされて、ユーザがユーザデータを用いて作業できる環境を電子計算機上に確保する。

[0043] 制御プログラムのインストールが正常に行われたかの判定を行う(ステップ16)。電子計算機、その上で動作するOSの設定によっては、外部からプログラム等のインストールができない場合がある。この場合は、制御プログラムのインストールが行われないので、電子データ管理装置1をこの電子計算機で利用することができない(ステップ17)。

[0044] 制御プログラムが電子計算機に正常にインストールされると、スイッチ10が第1メモリ6への切り替えを行い、第1メモリ6を電子計算機から利用可能になる(ステップ18)。第1メモリ6には、ユーザデータが保存されており、電子計算機へ転送することが可能になる。また、電子計算機上のアプリケーションプログラムから第1メモリ6へアクセスしユーザデータを呼び出すなどの作業を行うことができるようになる(ステップ19)。

[0045] また、同時に電子計算機にインストールされている制御プログラムが、履歴情報などのデータを第1メモリ6に書き込むことができるようになる。履歴情報には、ユーザデータを利用した履歴、ユーザデータを利用して作成したファイルの履歴、キーボード入力、マウス操作等の電子計算機を操作した履歴、通信回線を利用して電子計算機と周辺デバイスとのやりとりの履歴などが含まれても良い。USBコネクタ4が電子計算機から切断されると(ステップ20)、電子計算機にインストールされている制御プログラムが電子計算機内のユーザデータを削除する(ステップ21)。

[0046] このとき、制御プログラムはユーザデータを利用し、加工して作ったデータ、ファイルの削除を行っても良い。そして、電子計算機にインストールされた制御プログラムが自動消滅する(ステップ22)。このように、電子データ管理装置1を利用するとき、電子計算機上にはユーザデータ、及びこのユーザデータを利用して作成されたファイルが残ることがない。また、制御プログラムは、履歴情報等のデータを制御プログラム自体が動作している電子計算機のハードディスク又はRAMメモリ等の記憶媒体に記録しておいて、一定時間又は一定データ量になったら第1メモリ6又はネットワーク回線で別の電子計算機に転送して書き込みを行っても良い。また、同様に、制御プログラムは、履歴情報等のデータを電子計算機に接続されているMO、フレキシブルディスクやフラッシュメモリ等の記録媒体に書き込みしても良い。

[0047] 電子データ管理装置1を利用するためには、ユーザ又は管理者は電子データ管理

装置1を利用できるユーザの識別データを認証用データベース11に予め登録しておく。電子データ管理装置1のデータは通常のインターフェースでアクセスできない状態になっている。電子データ管理装置1へのアクセスがロックされていて、ユーザ認証が正常に行われて、利用許可のあるユーザのみが電子データ管理装置1を利用することができる。そのとき、電子データ管理装置1のアクセスロックが解除されて、電子計算機へのアクセス、コネクタの接続が行われる。

[0048] 〔実施の形態2〕

図5は、本発明の実施の形態2のシステムの動作の概要を図示したフローチャートである。本発明の実施の形態2は、上述の本発明の実施の形態1と基本的に同じであり、以下その本発明の実施の形態1と違う機能、処理のみを説明する。

ユーザ又は作業者は、ユーザデータ、ユーザの指紋情報などの識別データが登録された電子データ管理装置1を、使用する電子計算機に接続する(ステップ100)。認証モジュール12がユーザの認証を指紋情報入力部3からの指紋情報データを用いて行う(ステップ101)。認証モジュール12は、ユーザの指紋情報データを、電子データ管理装置1内に予め登録した識別データと比較して正当なユーザであるかを判定する(ステップ102)。

[0049] ユーザの指紋情報データが、認証用データベース11に格納されている識別データと一致しない場合は、認証モジュール12は利用許可がないユーザと判定し再度ユーザ認証を行う(ステップ103)。これは、電子データ管理装置1が電子計算機から切断されるか、ユーザ認証が成功するまで続く。ユーザの指紋情報データが、認証用データベース11に格納されている識別データと一致した場合は、認証モジュール12は正当なユーザであると判定し、次の処理に移る。

[0050] 認証モジュール12は、電子データ管理装置1をアンロックにし(ステップ104)、PnP機能が有効になり、PnP機能が開始する(ステップ105)。PnP機能を利用して、電子計算機が電子データ管理装置1を自動認識する。電子計算機が電子データ管理装置1を自動認識し終わると、通常の外付けメモリと同様にアクセスできるようになる(ステップ106)。

[0051] 電子データ管理装置1のUSBコネクタが電子計算機から切断されると(ステップ10

7)、電子計算機と電子データ管理装置1との一連のデータの送受信が終了する。この実施の形態2では、電子計算機に転送され、書き込まれたデータに関しては特別に制限を設けていない。ユーザは電子データ管理装置1にユーザデータを記録して持ち出し、それにアクセスできるユーザの認証を行ってからアンロックし、電子データ管理装置1に記録されているユーザデータのみにアクセスする許可をしている。

[0052] 〔実施の形態3〕

図6には、本発明の実施の形態3のシステムの動作の概要を図示している。本発明の実施の形態3のシステムは、上述の本発明の実施の形態1、2のシステムと基本的に同じであり、以下、本発明の実施の形態1、2のシステムと違う機能、処理のみを説明する。本実施の形態3のシステムは、配布元と使用者からなるシステムに関し、使用者は配布元のデータを用いて作業を行い、その結果を配布元に報告するものである。また、配布元は提供するデータを配布元が指定した特定の制限範囲のみ使用できる環境も提供している。

[0053] 図6には、電子データ管理装置1(以下、ハードウェアという)を提供する配布元、それを使用する使用者とのやりとりの流れを図示している。配布元は、ファイルシステムの機能を拡張した拡張ファイルシステムを提供する(ステップ200)。

[0054] 拡張ファイルシステムは、使用者が利用したアプリケーションプログラムの履歴、データの読み取り・編集・書き込みの履歴、ファイルの読込み・書き込み・複製・作成・削除などの履歴を取り記録する機能を有する。また、電子計算機のファイルシステムが提供する機能を制限する機能も有する。更に、ユーザのキーボード入力の履歴、マウスのクリック等のマウスを操作する履歴を取る機能も有する。

[0055] 使用者は、この拡張ファイルシステムを導入する(ステップ201)。この拡張ファイルシステムの導入は、使用者から配布元に申請する形で行われる。配布元は、ハードウェアを提供する(ステップ202)。それと同時に、ハードウェアと連携して動作するユーティリティの提供も可能である。拡張ファイルシステムとユーティリティの提供は、通常CD等の記録媒体に格納して行う。使用者は、使用するアプリケーションプログラムを配布元に申請し(ステップ203)、配布元はアプリケーションプログラムに対するハードウェア固有のファイルとデータを使用者に提供する(ステップ204)。

[0056] アプリケーションプログラムに対するハードウェア固有のファイルとデータは、ハードウェアに格納されている。使用者から配布元に拡張ファイルシステムの導入、アプリケーションプログラム等の使用許可を取るための申請は、インターネットを介して配布元のホームページからオンラインで行われても良い。又は、電子メールや紙媒体で申請が行われて同様な効果を発揮しても良い。

[0057] 使用者は、拡張ファイルシステムとユーティリティを電子計算機にインストールし、受け取ったハードウェアを電子計算機に接続する(ステップ205)。ハードウェアが電子計算機に接続されると、拡張ファイルシステムがハードウェアを認識し、制御モードに入る(ステップ206)。制御モードに関する情報は、配布元が提供したハードウェア固有のファイルに含まれている。

[0058] 使用者が、配布元のデータを利用して作業を行う。これらの作業の履歴が記録される(ステップ207)。ファイル使用履歴は、ハードウェアに記録される(ステップ208)。作業が終了すると、「作業の完了」の通知を配布元に送信する(ステップ209)。配布元はこの「作業の完了」通知を受け取る(ステップ214)。

[0059] そして、履歴データを配布元に送信する(ステップ210)。配布元は、履歴データを受信し(ステップ215)、受信したら応答する(ステップ216)。拡張ファイルシステムがこの応答を受信したら、複製ファイル、作業ファイル、そのデータ等を削除する(ステップ211)。そして、制限モードを解除し、通常のファイルシステムのモードに入る(ステップ212)。

[0060] これらの一連の作業が終了すると、使用者はハードウェアを配布元に返す(ステップ213)。配布元は、履歴データを受信してから、使用者が履歴データを解析して(ステップ217)、提供ファイル、データを正確に使用したかを把握することができる。また、配布元は、返却されてハードウェア内に保存されている履歴データを解析して把握することも可能である(ステップ218)。

[0061] 配布元に送信される通知、配布元からの応答は、インターネット等の通信回線によってダイレクトで行われる。使用者から配布元への履歴データなどの送信は専用通信回線、インターネット、公衆通信網などの通信網によって行われる。使用者と配布元が通信網で接続されてない場合は、ハードウェアにそれらの履歴を保存してハー

ドウェアを返却することによって行われる方法であっても良い。

[0062] 〔実施の形態4〕

図7には、本実施の形態4のシステムの機能の概要を図示している。本発明の実施の形態4のシステムは、上述の本発明の実施の形態1ー3のシステムと基本的に同じであり、以下、本発明の実施の形態1ー3のシステムと違う機能、処理のみを説明する。本実施の形態4のシステムでは制御プログラムが電子計算機にインストールされて、ユーザが使用するアプリケーションプログラムを登録できるようになっている。

[0063] ユーザは、制御プログラムをインストールするとき、アプリケーションプログラム、特定のデータ、ファイルを登録し、その登録されたアプリケーションプログラム、特定のデータ、ファイルを使用した履歴を取得し、登録されたアプリケーションプログラムの使用範囲を制限することが可能になり、その使用履歴を追跡して把握することが可能になる。

[0064] ユーザは、電子データ管理装置1を電子計算機と接続して、ユーザ認証が行われる(ステップ301)。ユーザ認証が完了すると、電子データ管理装置1のアクセスロックが解除されて電子計算機と電子データ管理装置1とのやり取りできるようになり、OSのPnP機能が有効になる。よって、電子データ管理装置1がPnP機能によって電子計算機に認識されて、電子データ管理装置1のドライバのインストールが開始される(ステップ302)。電子データ管理装置1のドライバのインストール終了後は、制御プログラムのインストールが開始される(303)。

[0065] このとき、ユーザはアプリケーションプログラムの登録をすることが可能である(ステップ304)。ユーザがアプリケーションプログラムの登録をしない場合は、制御プログラムのインストールが続けて行われる(ステップ306)。ユーザがアプリケーションプログラムの登録を行う場合は、登録するアプリケーションプログラムを選択し、そのファイル名、パス、ディレクトリなどを指定、選択して登録を行う(ステップ305)。

[0066] アプリケーションプログラムの登録が終わると、制御プログラムのインストールが続けて行われる(ステップ306)。制御プログラムが正常にインストールされたかを確認して電子データ管理装置1の使用が可能になる(ステップ307、308、309)。

[0067] また、上述のようにユーザが制御プログラムをインストールするときアプリケーション

プログラムを登録し、その使用履歴を取得し、登録されたアプリケーションプログラムの使用範囲を制限することが可能である。アプリケーションプログラムの他に特定のデータ、ファイルを登録しても良い。データ、ファイルを登録すると、実施の形態1のシステムのようにデータ、ファイルの使用履歴を追跡して把握することが可能になる。ユーザは、制御プログラムを使用中でも、アプリケーションプログラム、データ、ファイルの登録、登録の取り消しをすることも可能である。

[0068] 〔実施の形態5〕

図8には、本発明の実施の形態5のシステムの動作の概要を図示している。本発明の実施の形態5のシステムは、上述の本発明の実施の形態1ー4のシステムと基本的に同じであり、以下、本発明の実施の形態1ー4のシステムと違う機能、処理のみを説明する。本実施の形態5のシステムでは、電子データ管理装置1が電子計算機から切断されても制御プログラムを継続して使用することが可能なものを提供している。電子データ管理装置1が実施の形態1ー4のシステムに示すように電子計算機に接続され、電子データ管理装置1内の制御プログラムがインストールされて使用されている。

[0069] USBコネクタが電子計算機から切断される(ステップ350)。そのとき、制御プログラムのアンインストールを開始するかを確認する(ステップ351)。アンインストールしない場合は、電子データ管理装置1を継続して使用できる(ステップ356)。ユーザは、電子データ管理装置1を再度電子計算機に接続するとき、切断前の環境が電子計算機に残っているので制御プログラムを再度インストールする必要はない。アンインストールを開始するときは、今まで使用したデータを削除するかを確認し(ステップ352)、電子計算機内のデータを削除する(ステップ353)。そして、制御プログラム自身を削除するかを確認する(ステップ354)。

[0070] データと制御プログラムを削除しない場合は、それぞれ続けて電子データ管理装置1を使用する(ステップ356)。ただし、制御プログラムの削除を行った場合は、継続して電子データ管理装置1を使用することができない(ステップ355)。電子データ管理装置1を継続して使用するとは、電子データ管理装置1を再び電子計算機に接続して使用することが可能である。そのとき、既にインストールされた制御プログラムを続

けて使用することが可能である。

[0071] 〔実施の形態6〕

本実施の形態6は、電子データ管理装置1の他の実施の形態である。本発明の実施の形態6の電子データ管理装置20は、上述の本発明の実施の形態1ー5のシステムで用いる電子管理装置1と基本的に同じであり、以下、本発明の実施の形態1ー5の電子管理装置1と違う機能、処理のみを説明する。図9には、本実施の形態6の電子データ管理装置20の概要を図示している。電子データ管理装置20は、筐体2、筐体2の一辺に設けた押しボタン式のキー21、そしてコネクタ4から構成されている。

[0072] 電子データ管理装置20は、実施の形態1ー5の電子データ管理装置1とはユーザ認証には暗証番号を利用している点が異なる。その他の機能は、前述した電子データ管理装置1と同様であり、詳しい説明は省略する。違っている部分の説明だけを行う。ユーザは、電子データ管理装置20のロックを解除するために、その一辺に設けている押しボタン式のキー21から暗証番号を入力する。

[0073] 暗証番号を入力するときに、その入力開始、入力終了を識別するために「＃」、「＊」などの決められた記号キーを暗証番号入力の前後に押しても良い。押しボタン式のキー21は0ー9までの数字、一部の記号のボタンを有しているが、電子データ管理装置20の大きさ、用途に合わせてボタンの数を増減しても良い。

[0074] 電子データ管理装置20の内部構造は図2と同様であり、ユーザ認証は認証モジュール12が行い、その認証のためにはあらかじめ登録された暗証番号が認証用データベース11に記憶されている。

[0075] この電子データ管理装置20を利用するまでの手順は、図10のフローチャートに示している。専用のアプリケーションプログラムでユーザデータを電子データ管理装置20の第1メモリ6に書き込み、暗証番号を認証用データベース11に登録する(ステップ401、402)。よって、電子データ管理装置20が利用可能になる。

[0076] 〔実施の形態7〕

本実施の形態7は、電子データ管理装置1の他の実施の形態である。本発明の実施の形態7の電子データ管理装置30は、上述の本発明の実施の形態1ー5のシステムで使用する電子データ管理装置1又は電子データ管理装置20と基本的には同一

であり、以下、本発明の実施の形態1ー5のシステムと違う機能、処理のみを説明する。図11は、本実施の形態7の電子データ管理装置30の外観を示す図である。錠32と鍵31の組を用いたユーザ認証を行う電子データ管理装置30の概要を図している。電子データ管理装置30は、筐体2、筐体2の一辺に設けた錠32、そしてコネクタ4から構成されている。

[0077] 伝統的に使用されている機構的な錠を使用するものであり、錠32とこの錠32を開閉するための鍵31が1組になって電子データ管理装置30に付属されている。正当な鍵31を用いて錠32に挿入して回転させると、接点等により電気的にこれを検知して、正当なユーザーであることを認識するものである。電子データ管理装置30の内部構造は図2と同様であり、ユーザ認証は認証モジュール12が行う。ユーザ認証は、錠32の開閉によって行われるので、認証用データベース11が不要である。実施の形態1ー5の電子データ管理装置1とはユーザ認証に錠32と鍵31の組を利用している点が異なる。その他の機能は、前述の電子データ管理装置1と同様であり、詳しい説明は省略する。異なる部分の説明だけを行う。

[0078] ユーザは、電子データ管理装置30のロックを解除するために、その一辺に設けている錠32に矢印33の方向で示すように鍵31を差し込んで錠32のロックを解除する。この情報を、認証モジュール12が察知し、電子データ管理装置30のアクセスロックを解除し、電子データ管理装置30へのアクセスが可能になる。

[0079] 〔実施の形態8〕

図12、13には、本発明の実施の形態8のシステムの動作の概要を図示している。本発明の実施の形態8は、上述の本発明の実施の形態1ー5のシステムと基本的に同じであり、以下、本発明の実施の形態1ー5のシステムと違う機能、処理のみを説明する。本実施の形態8のシステムでは、電子データ管理装置1が電子計算機から切断されても制御プログラムを継続して使用可能なものを提供している。

[0080] 電子データ管理装置1が実施の形態1ー5のシステムに示すように電子計算機に接続され、電子データ管理装置1内の制御プログラムがインストールされて使用されている。図12のフローチャートに示すように、USBコネクタ4が電子計算機から切断される(ステップ450)。そのとき、アンインストールを開始するかを確認する(ステップ45

1)。アンインストールしない場合は、電子データ管理装置1を継続して使用できる(ステップ458)。ユーザは、電子データ管理装置1を再度電子計算機に接続するとき切断前の環境が電子計算機に残っているので制御プログラムを再度インストールする必要はない。

[0081] アンインストールを開始するときは、今まで使用したユーザデータを削除するかを確認し(ステップ452)、制御プログラムは電子計算機内のユーザデータを削除する(ステップ453)。ユーザデータを削除しない場合は、ステップ453がスキップされる(ステップ458)。そして、制御プログラムを無効にするかを確認する(ステップ454)。

[0082] 制御プログラムを無効にする場合は、制御プログラムを無効にする作業を行う(ステップ459)。これによって、制御プログラムは無効になり、電子計算機は通常のものと変わらない動作をするようになる(ステップ457)。言い換えると、制御プログラムはインストールされているが活動しない無効な状態になる。制御プログラムを無効にしない場合は、制御プログラム自身を削除するかを確認する(ステップ455)。制御プログラムを削除しない場合は、続けて制御プログラムを使用する(ステップ458)。

[0083] 制御プログラムの削除を行った場合は、電子計算機は通常のものと変わらない動作をするようになる(ステップ457)。電子データ管理装置1を継続して使用するときは、電子データ管理装置1を再び電子計算機に接続して使用することが可能である。そのとき、既にインストールされた制御プログラムを続けて使用することが可能である。

[0084] 図12のフローチャートでは、使用したユーザデータの削除(ステップ452)、制御プログラムの無効(ステップ454)を確認している別の例を図示している。図12と同様のステップ番号がついているものはその説明を上記に行っているので以下は省略する。図13には、制御プログラムの無効(ステップ470)、制御プログラムの削除(ステップ471)を確認した後に使用したユーザデータの削除(ステップ476、472)をそれぞれ確認している。

[0085] 使用したユーザデータの削除(ステップ476、472)をそれぞれ確認した後、又はユーザデータの削除を行った後(ステップ477、473)に制御プログラムの無効(ステップ478)、制御プログラムの削除(ステップ471)を行っている。本発明の実施の形態8は、本発明の実施の形態1ー5のシステムのユーザの指紋によるユーザ認証を前提

にしているが、本発明の実施の形態6，7に示すようなユーザ認証を行うことも可能である。

[0086] 本発明の実施の形態は、これまでに記述したような実施の形態1から8のシステムのみに適用され利用されるものではなく、同様な効果が得られるどのような形式・形態でも利用しても良い。

産業上の利用可能性

[0087] 本発明は、ユーザのファイルやデータなどを携帯可能なメモリ装置に記録して搬送して使用することが可能であり、セキュリティが必要な業界で利用すると良い。特に、営業または経理データ等でユーザデータやファイルなどの秘密情報の提供が必要とされる印刷業界、販売店で利用されることが望ましい。また、ペーパーレス処理を行うための機関、顧客へのファイル提供などに利用されても良い。音楽配信、映像配信、電子出版などの電子コンテンツ配信サービスを行うとき、被受信者を特定し、被受信者のメモリに電子コンテンツを書き込んで提供するときに利用されても良い。

図面の簡単な説明

[0088] [図1]図1は、電子データ管理装置1の外観を示す外観図である。

[図2]図2は、電子データ管理装置1の基板5の構成を示す機能である。

[図3]図3は、電子データ管理装置1を利用する前の準備の手順を示すフローチャートである。

[図4]図4は、電子データ管理装置1を利用する全体の流れを示すフローチャートである

[図5]図5は、本発明の実施の形態2のシステムの動作の概要を図示したフローチャートである。

[図6]図6は、本発明の実施の形態3のシステムの動作の概要を図示したフローチャートである。

[図7]図7は、本発明の実施の形態4のシステムの動作の概要を図示したフローチャートである。

[図8]図8は、本発明の実施の形態5のシステムの動作の概要を図示したフローチャートである。

[図9]図9は、暗証番号を用いて認証を行う実施の形態6の電子データ管理装置20の外観を示した外観図である。

[図10]図10は、電子データ管理装置20の利用する準備の手順を示すフローチャートである。

[図11]図11は、鍵を用いて認証を行う実施の形態7の電子データ管理装置30の外観を示した外観図である。

[図12]図12は、本発明の実施の形態8のシステムの動作の概要を図示したフローチャートである。

[図13]図13は、本発明の実施の形態8のシステムの動作の他の例を図示したフローチャートである。

符号の説明

[0089] 1…電子データ管理装置

2…筐体

3…指紋認証部

4…USBコネクタ

5…基板

6…第1メモリ

7…第2メモリ

8…CPU

9…バスコントローラ

10…スイッチ

11…指紋認証用データベース

12…指紋認証部

20…電子データ管理装置

21…押しボタン式入力部

30…電子データ管理装置

31…鍵

32…錠

請求の範囲

[1] データを記憶するデータ記憶手段(6)と、

認証用の識別データが登録されている識別データ記憶手段(11)と、

ユーザの認証情報を入力する入力手段(3, 21, 31, 32)と、

前記入力手段(3, 21, 31, 32)からの入力データと、前記識別データ記憶手段(11)に登録された前記識別データとを比較して前記ユーザの認証を行う認証手段(12)と、

電子計算機と接続して前記データの送受信を行うインターフェース手段(9)と

を備え、

前記認証の結果、前記入力データと前記識別データが一致するときに前記データへのアクセスを許可する電子データ管理装置(1, 20, 30)において、

制御プログラムを記憶するプログラム記憶手段(7)を有し、

前記認証手段(12)によって前記ユーザが認証された後、前記制御プログラムが前記電子計算機にインストールされ、前記電子計算機から前記データを読み出しすることが可能になる

ことを特徴とする電子データ管理装置。

[2] 請求項1において、

前記制御プログラムは、前記認証手段(12)による前記認証が完了した後、前記電子データ管理装置(1, 20, 30)のロックが解除されて、接続されている前記電子計算機が前記電子データ管理装置(1, 20, 30)の自動認識を開始する

ことを特徴とする電子データ管理装置。

[3] 請求項1において、

前記データ記憶手段(6)と前記プログラム記憶手段(7)とを選択的にスイッチするスイッチ制御手段(10)を有する

ことを特徴とする電子データ管理装置。

[4] 請求項1又は3において、

前記電子計算機から前記データ記憶手段(6)に書き込みすることが可能で、前記制御プログラムにより前記電子計算機で前記データを操作した履歴、又は前記電子

計算機の前記データを操作した履歴が前記データ記憶手段(6)に書き込まれることを特徴とする電子データ管理装置。

[5] 請求項1又は2において、

前記識別データは指紋データであり、

前記入力手段(3)から前記ユーザの指紋情報を入力し、

前記認証手段(12)により前記ユーザの指紋認証を行う

ことを特徴とする電子データ管理装置。

[6] 請求項1又は2において、

前記識別データは登録暗証番号であり、

前記入力手段(21)から暗証番号を入力し、

前記認証手段(12)により前記暗証番号と前記登録暗証番号と比較して前記ユーザの認証を行う

ことを特徴とする電子データ管理装置。

[7] 請求項1又は2において、

前記認証手段(12)は、機構的な錠(32)と鍵(31)を有し、

前記鍵(31)を持っている前記ユーザに前記データへのアクセスを許可する

ことを特徴とする電子データ管理装置。

[8] 登録された認証用情報を記憶する認証用情報領域(11)と、

ユーザの識別情報を入力する入力部(3, 21, 31, 32)と、

前記認証用情報と、前記識別情報とを比較して前記ユーザの認証を行うための認証機能を有する認証部(12)と、

データを記憶するデータ記憶領域(6)と、

制御プログラムを記憶するプログラム記憶領域(7)と

を有し、

電子計算機と接続されると前記認証部(12)によって前記ユーザの前記認証を行い、前記認証が完了すると、前記ユーザには前記データ記憶領域(11)にアクセスする許可を与える電子データ管理装置において、

前記認証が行われた後に、前記制御プログラムが前記電子計算機にインストール

され、

前記電子計算機で前記データを利用して作業を行うとき、前記制御プグラムが前記作業の履歴を記憶するように前記電子計算機を動作させる

ことを特徴とする電子データ管理装置用制御プログラム。

[9] 請求項8において、

前記制御プログラムは、前記電子計算機と前記電子データ管理装置との前記接続が切断されると、前記制御プログラムが前記電子計算機内に送信された前記データを削除する

ことを特徴とする電子データ管理装置用制御プログラム。

[10] 請求項9において、

前記制御プログラムが、前記電子計算機と前記電子データ管理装置との前記接続が切断されるとき、前記制御プログラムに内蔵された消滅機能を備えた自動消滅プログラムにより自動消滅する機能を有する

ことを特徴とする電子データ管理装置用制御プログラム。

[11] 請求項8又は9において、

前記制御プログラムは、前記電子計算機内で動作をしない状態である無効機能を有する

ことを特徴とする電子データ管理装置用制御プログラム。

[12] 請求項8において、

前記制御プログラムは、

前記電子計算機で前記データを、複製、削除、編集、閲覧、読込み、及び書込み、から選択される一以上の履歴、又は前記データを用いて作成したファイル若しくは新規データの履歴を取得する履歴取得機能と、

前記履歴を前記データ記憶領域(6)に書き込みするデータ記録機能と、

通信手段を利用して前記履歴を送信する送信機能と

を有する

ことを特徴とする電子データ管理装置用制御プログラム。

[13] 請求項8又は12において、

前記履歴は、

前記電子計算機の入力手段から操作した操作履歴である

ことを特徴とする電子データ管理装置用制御プログラム。

[14] 請求項8において、

前記制御プログラムが、前記データを前記電子計算機内に特定アプリケーションで、又は任意に複製、削除、編集、閲覧、読込み、及び書込み、する操作から選択される一以上の操作だけをできるように前記電子計算機のファイルシステムに制限をする

ことを特徴とする電子データ管理装置用制御プログラム。

[15] 請求項8において、

前記制御プログラムが、前記電子計算機のOSの全命令を実行できるカーネルモードで動作する

ことを特徴とする電子データ管理装置用制御プログラム。

[16] 認証用情報を記憶する認証情報記憶部(11)と、

ユーザの認証情報を入力する入力部(3, 21, 31, 32)と、

前記入力部(3, 21, 31, 32)からのデータを用いて前記ユーザの認証を行う認証部(12)と、

データを記憶するデータ記憶部(6)と

を有する電子データ管理装置(1, 20, 30)を用いて、

電子計算機に接続されると前記認証部(12)によって前記ユーザの前記認証が行われ、前記認証情報記憶部(11)に登録された前記認証用情報と一致する前記認証情報を有する前記ユーザに前記データへのアクセスを許可する

データ管理方法において、

前記電子データ管理装置が、制御プログラムを格納するプログラム記憶部(7)を有し、

前記認証が終わると前記制御プログラムが前記電子計算機にインストールされ、

前記電子計算機で前記データを利用する利用環境を確保する

ことを特徴とする電子データ管理方法。

[17] 請求項16において、

前記利用環境は、前記電子計算機で動作する特定アプリケーションプログラムからのみ前記データへアクセスすることを許可する、制限である

ことを特徴とする電子データ管理方法。

[18] 請求項16において、

前記制御プログラムは、前記電子計算機の入力手段から操作する履歴、又は前記データを用いて複製、削除、編集、閲覧、読込み、及び書込み、する操作から選択される一以上の前記データへのアクセスの履歴、又は前記データを用いて作成したファイル若しくは新規データの履歴を残す機能を有する

ことを特徴とする電子データ管理方法。

[19] 請求項16において、

前記電子データ管理装置(1, 20, 30)と前記電子計算機との前記接続が切断されると、前記制御プログラムは、前記電子計算機内の前記データ、前記データの複製、前記データを利用して作成したデータ又はファイルの内の1つ以上を削除する

ことを特徴とする電子データ管理方法。

[20] 請求項16、18、19の中から選択される1項において、

前記制御プログラムが、前記制御プログラムに内蔵されている自動消滅機能を備えた自動消滅プログラムにより自動消滅する機能を有する

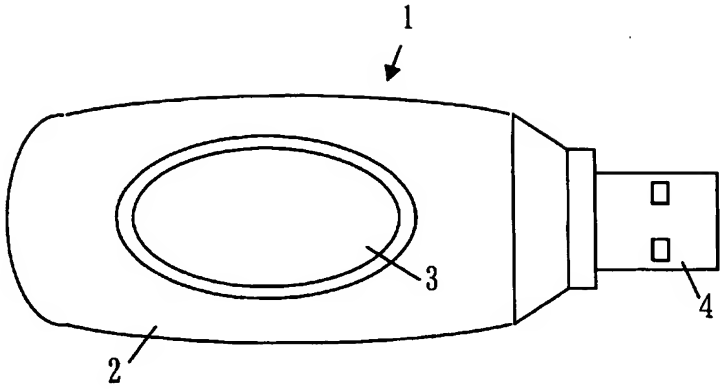
ことを特徴とする電子データ管理方法。

[21] 請求項16、18、19の中から選択される1項において、

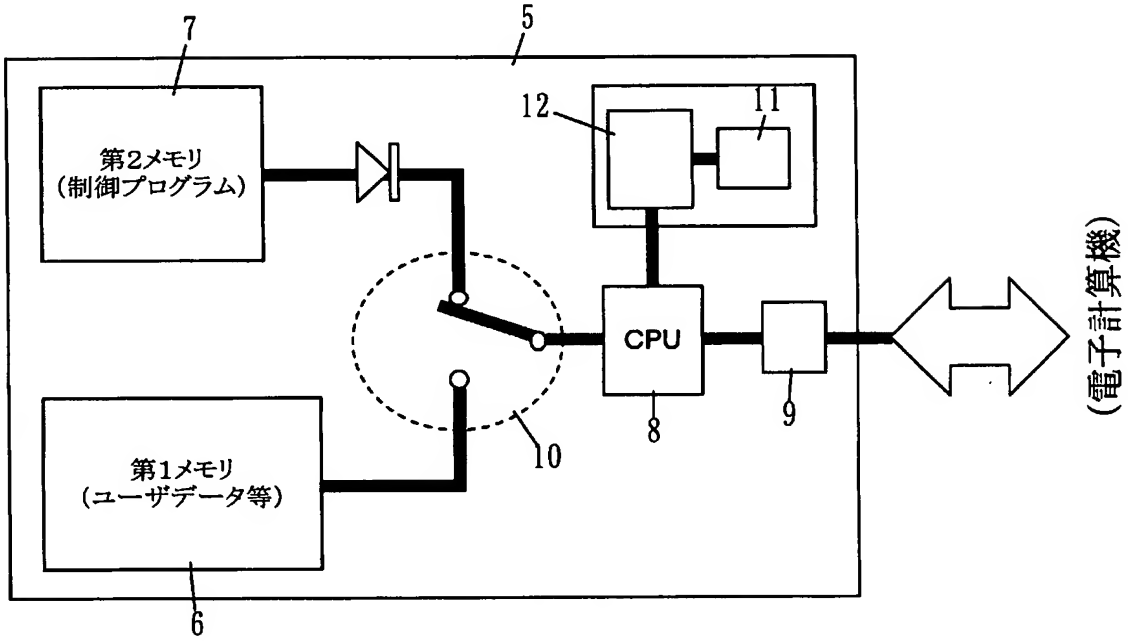
前記制御プログラムは、前記電子計算機内で機能をしない状態である無効機能を有する

ことを特徴とする電子データ管理方法。

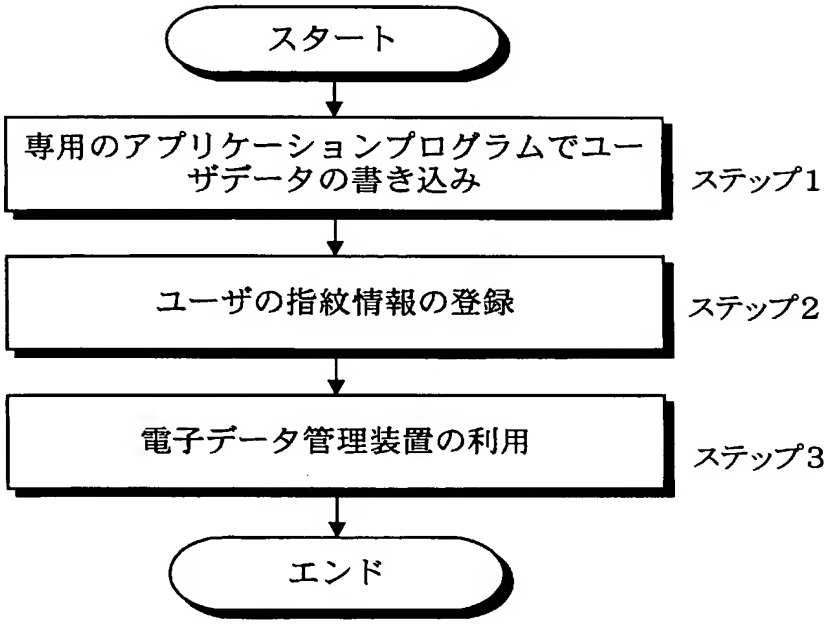
[図1]



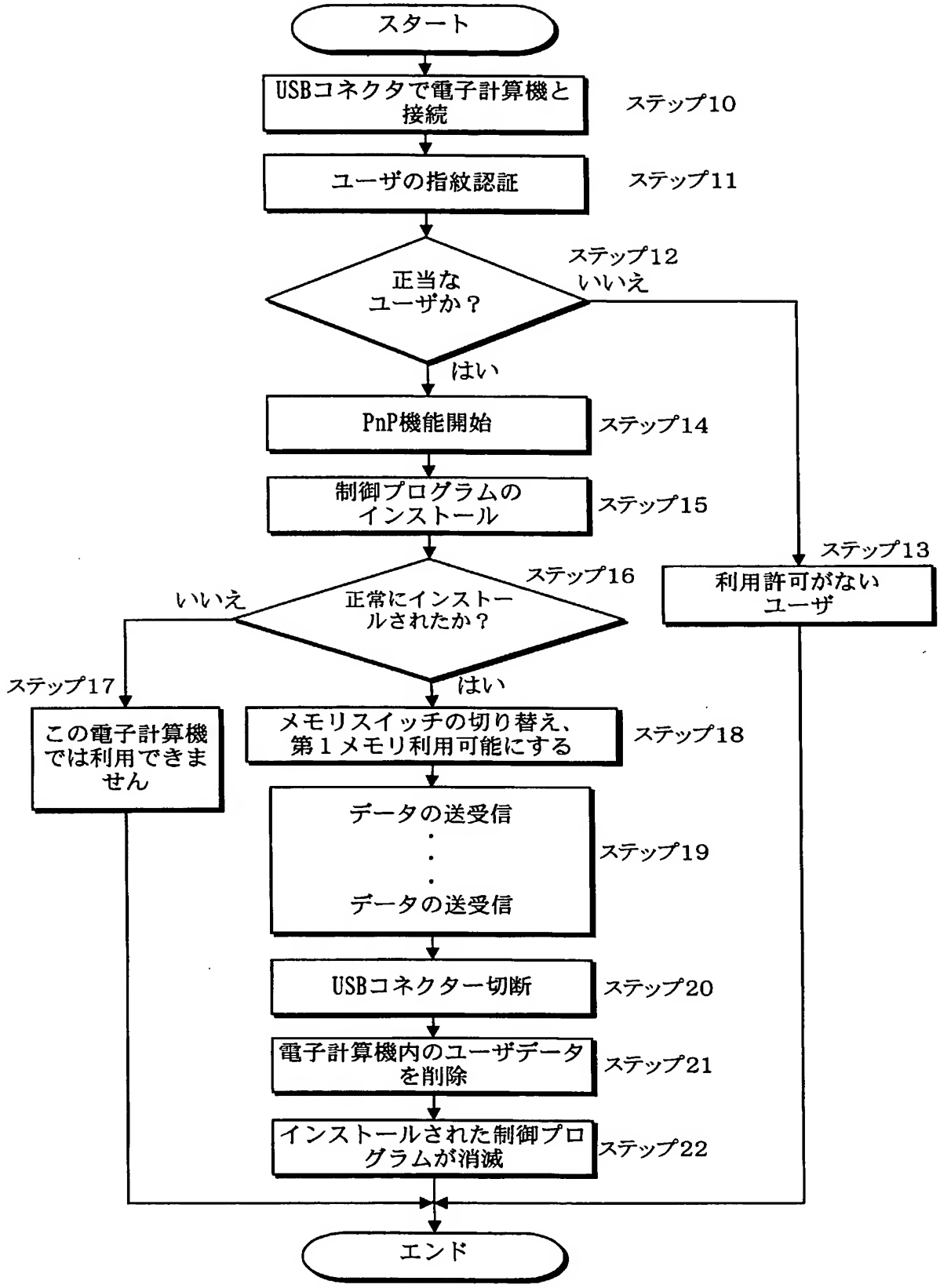
[図2]



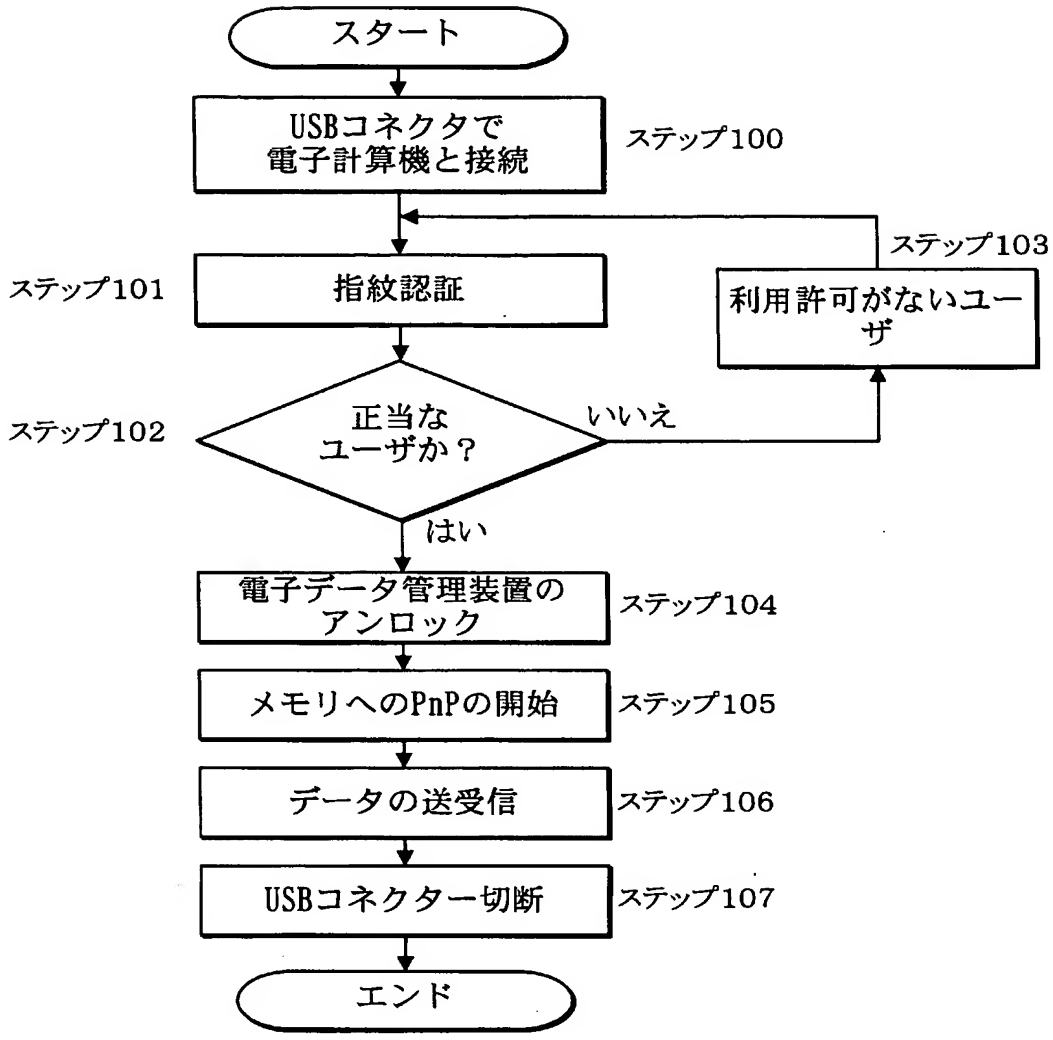
[図3]


スタート
専用のアプリケーションプログラムでユーザデータの書き込み
ステップ1
ユーザの指紋情報の登録
ステップ2
電子データ管理装置の利用
ステップ3
エンド

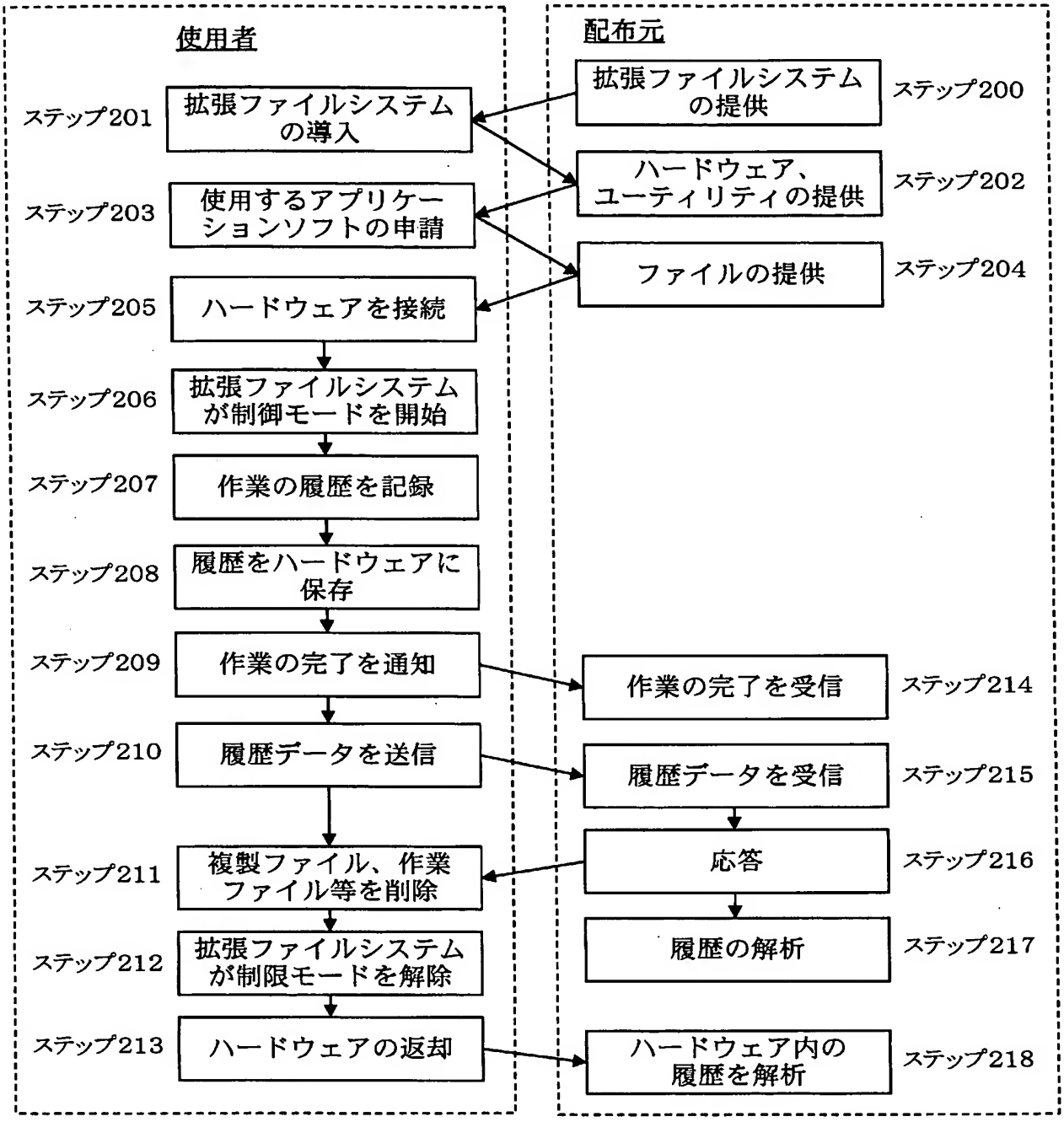
[図4]


スタート
USBコネクタで電子計算機と接続
ステップ10
ユーザの指紋認証
ステップ11
正当なユーザか？
ステップ12
いいえ
はい
PnP機能開始
ステップ14
制御プログラムのインストール
ステップ15
正常にインストールされたか？
ステップ16
いいえ
はい
ステップ13
利用許可がないユーザ
ステップ17
この電子計算機では利用できません
メモリスイッチの切り替え、第１メモリ利用可能にする
ステップ18
データの送受信
・
・
・
データの送受信
ステップ19
USBコネクター切断
ステップ20
電子計算機内のユーザデータを削除
ステップ21
インストールされた制御プログラムが消滅
ステップ22
エンド

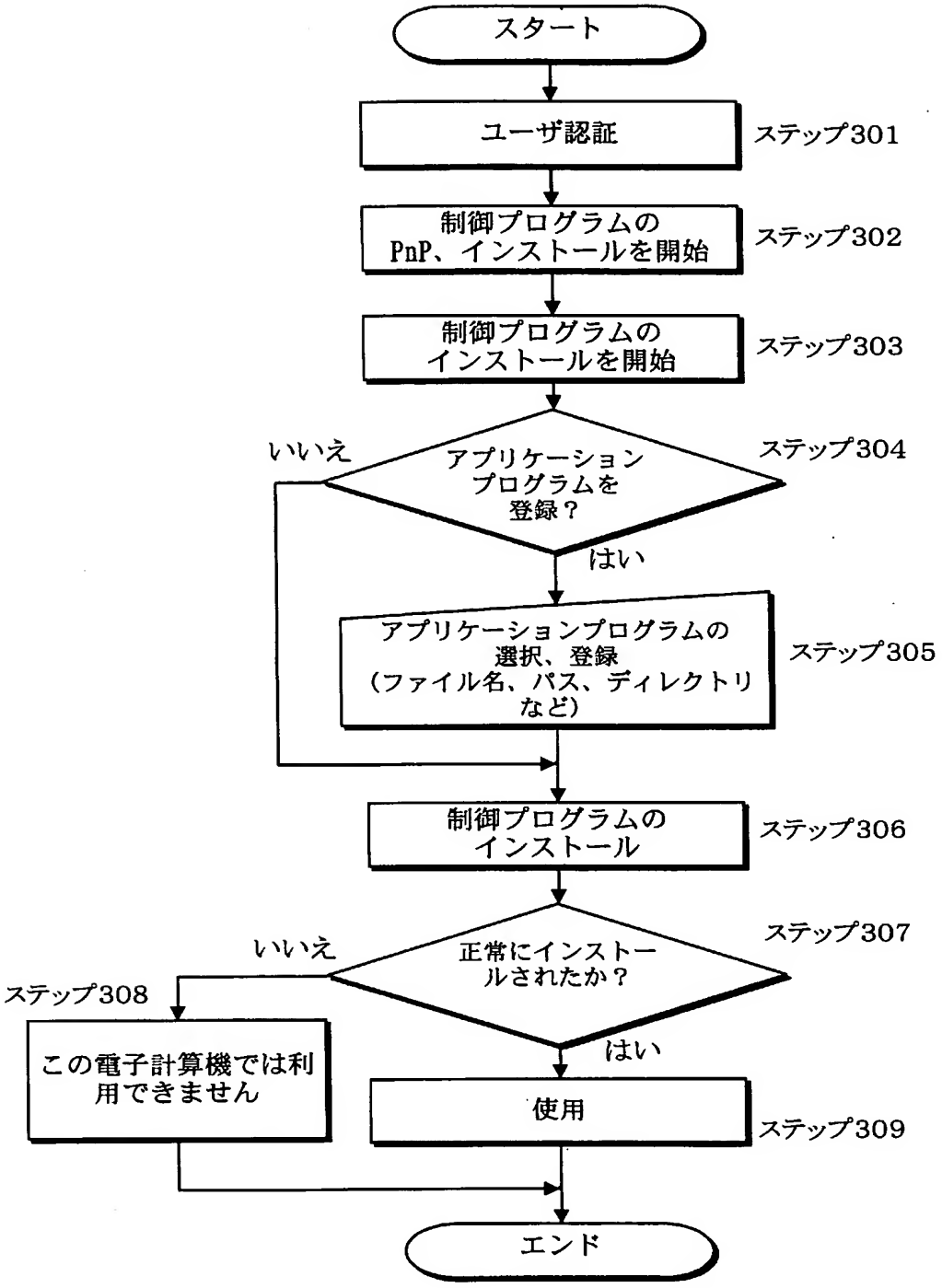
[図5]


スタート
USBコネクタで
電子計算機と接続
ステップ100
ステップ101
指紋認証
ステップ103
利用許可がないユーザ
ステップ102
正当な
ユーザか？
いいえ
はい
電子データ管理装置の
アンロック
ステップ104
メモリへのPnPの開始
ステップ105
データの送受信
ステップ106
USBコネクター切断
ステップ107
エンド

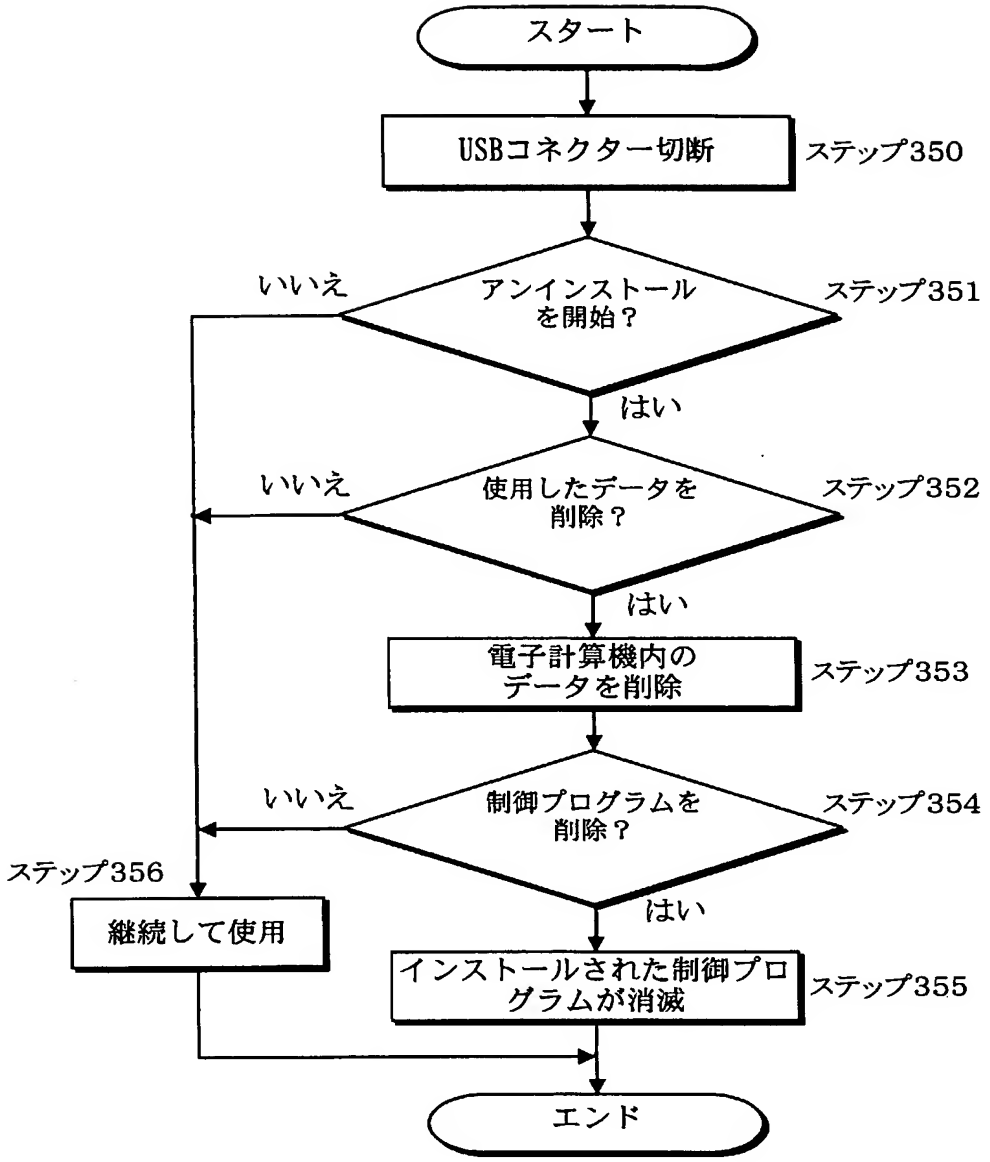
[図6]


使用者
配布元
拡張ファイルシステムの提供
ステップ200
ステップ201
拡張ファイルシステムの導入
ハードウェア、ユーティリティの提供
ステップ202
ステップ203
使用するアプリケーションソフトの申請
ファイルの提供
ステップ204
ステップ205
ハードウェアを接続
ステップ206
拡張ファイルシステムが制御モードを開始
ステップ207
作業の履歴を記録
ステップ208
履歴をハードウェアに保存
ステップ209
作業の完了を通知
作業の完了を受信
ステップ214
ステップ210
履歴データを送信
履歴データを受信
ステップ215
応答
ステップ216
ステップ211
複製ファイル、作業ファイル等を削除
履歴の解析
ステップ217
ステップ212
拡張ファイルシステムが制限モードを解除
ステップ213
ハードウェアの返却
ハードウェア内の履歴を解析
ステップ218

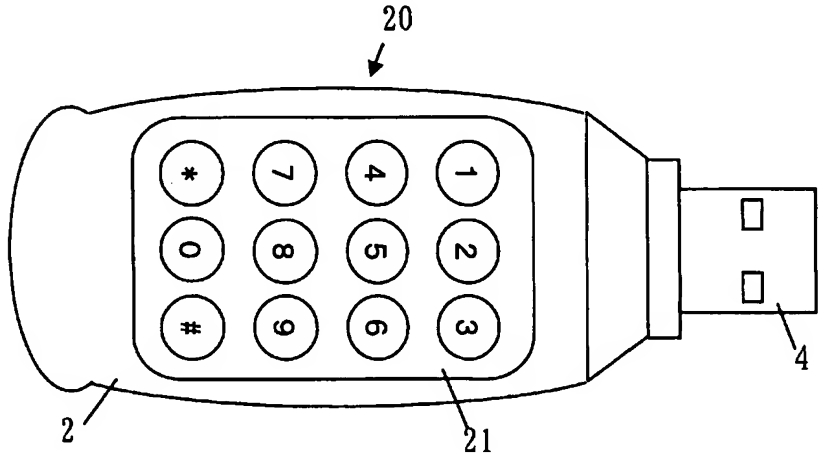
[図7]


スタート
ユーザ認証
ステップ301
制御プログラムの
PnP、インストールを開始
ステップ302
制御プログラムの
インストールを開始
ステップ303
いいえ
アプリケーション
プログラムを
登録？
ステップ304
はい
アプリケーションプログラムの
選択、登録
(ファイル名、パス、ディレクトリ
など)
ステップ305
制御プログラムの
インストール
ステップ306
いいえ
正常にインスト
ールされたか？
ステップ307
ステップ308
この電子計算機では利
用できません
はい
使用
ステップ309
エンド

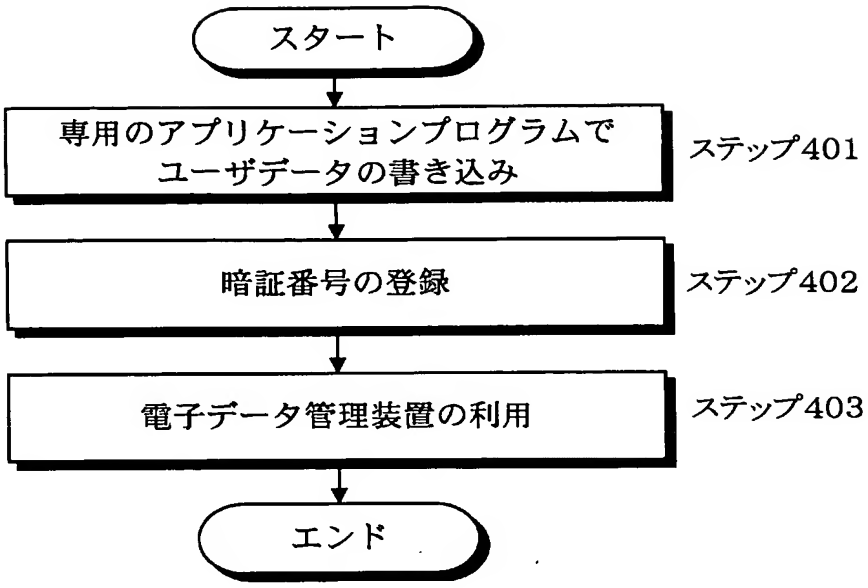
[図8]


スタート
USBコネクター切断
ステップ350
アンインストール
を開始？
いいえ
ステップ351
はい
使用したデータを
削除？
いいえ
ステップ352
はい
電子計算機内の
データを削除
ステップ353
制御プログラムを
削除？
いいえ
ステップ354
はい
ステップ356
継続して使用
インストールされた制御プロ
グラムが消滅
ステップ355
エンド

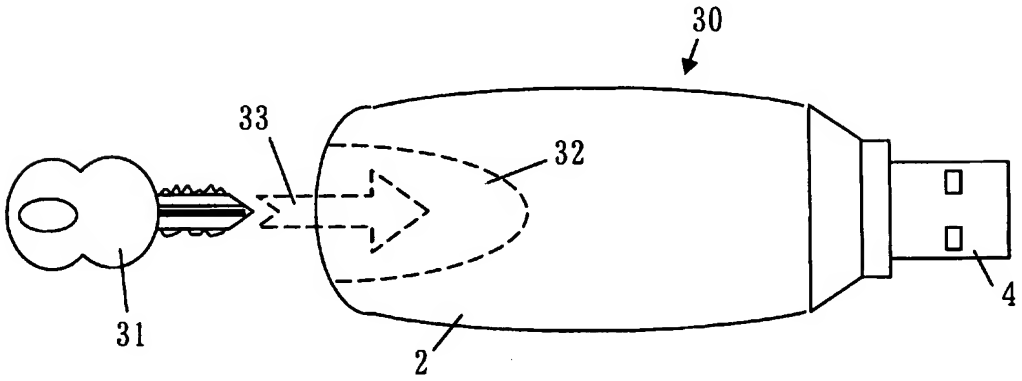
[図9]


20
*
7
4
1
0
8
5
2
#
9
6
3
4
2
21

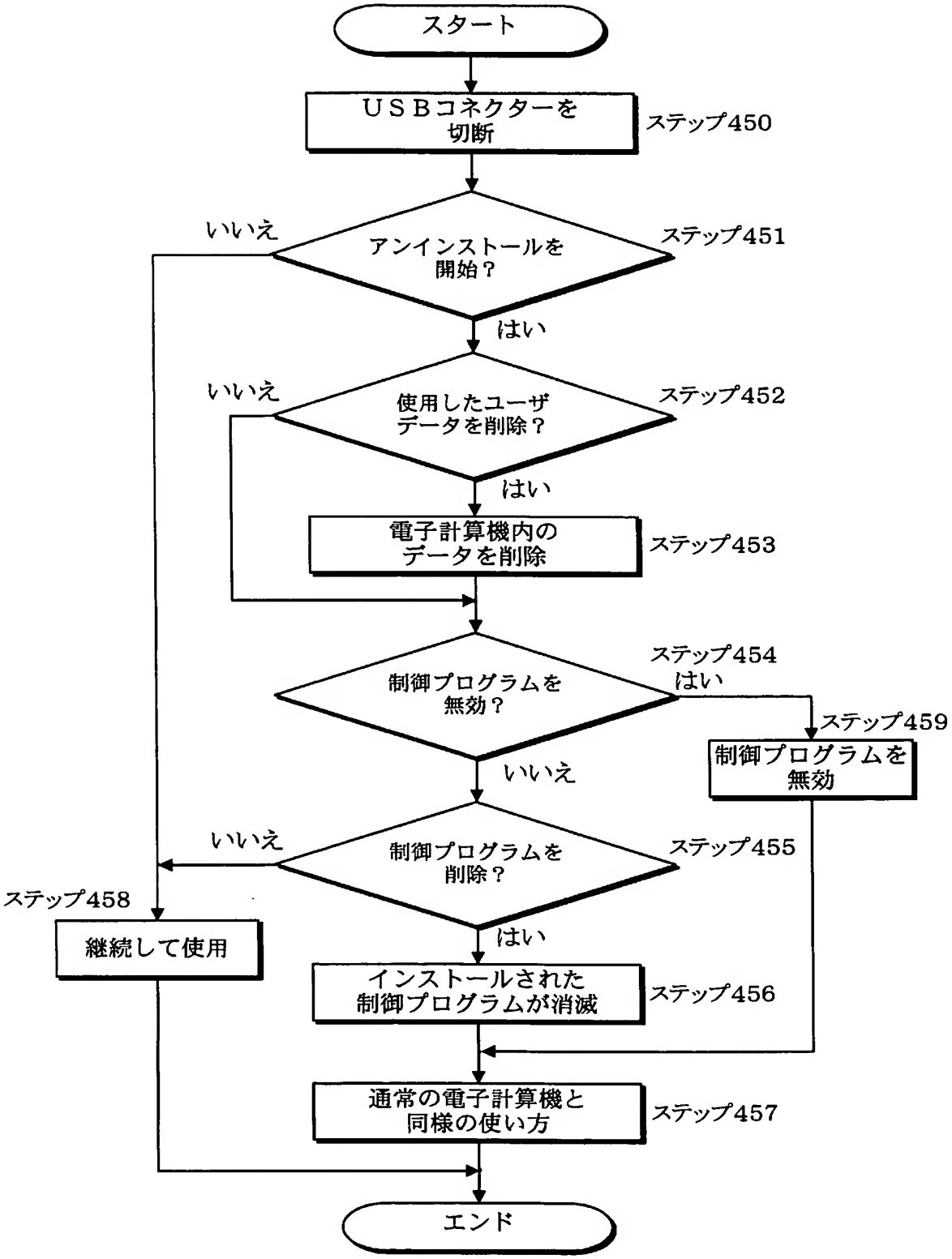
[図10]


スタート
専用のアプリケーションプログラムで
ユーザデータの書き込み
ステップ401
暗証番号の登録
ステップ402
電子データ管理装置の利用
ステップ403
エンド

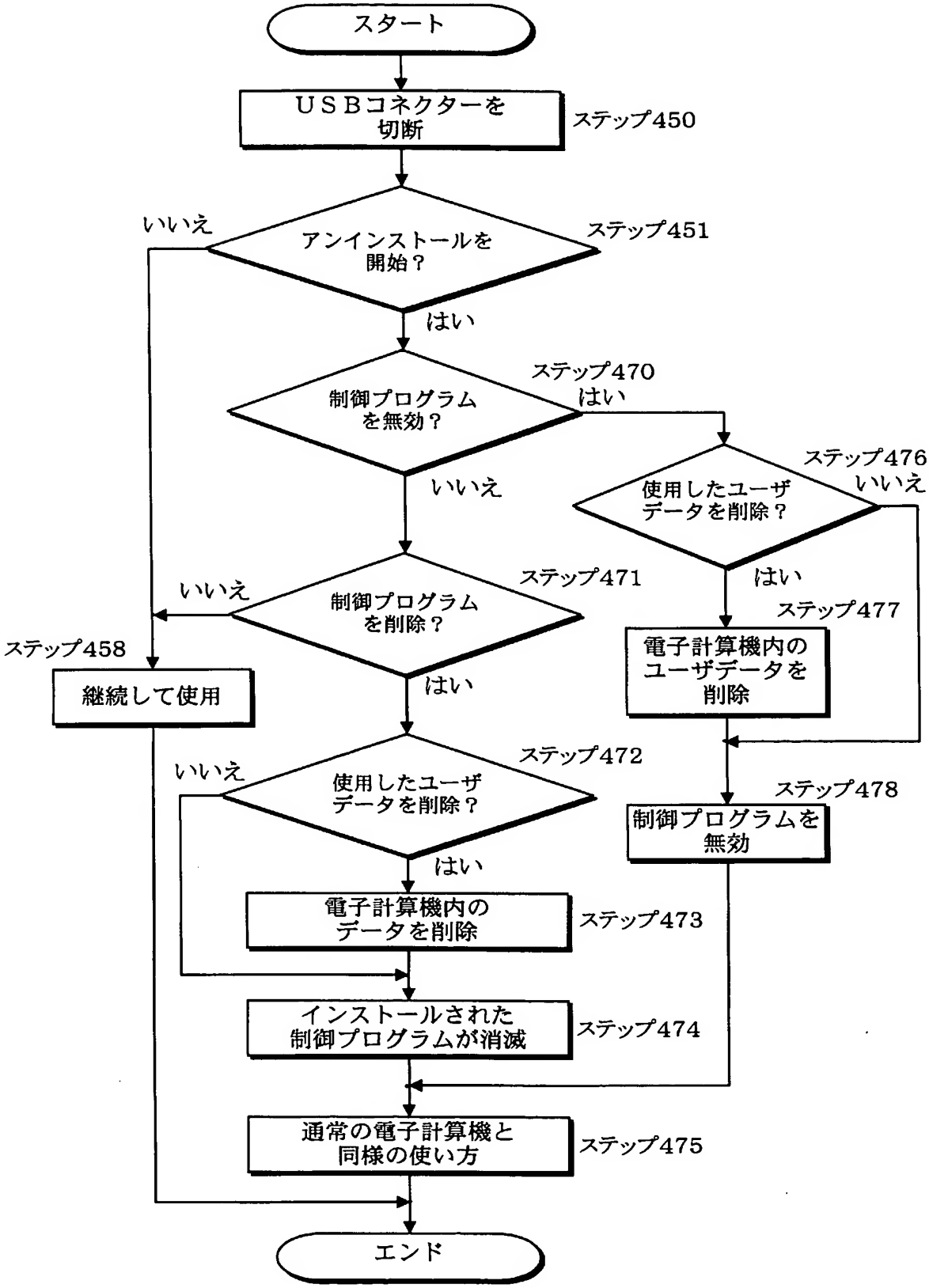
[図11]


30
33
32
31
2
4

[図12]


スタート
ＵＳＢコネクターを切断
ステップ450
アンインストールを開始？
いいえ
ステップ451
はい
使用したユーザデータを削除？
いいえ
ステップ452
はい
電子計算機内のデータを削除
ステップ453
制御プログラムを無効？
ステップ454
はい
ステップ459
制御プログラムを無効
いいえ
制御プログラムを削除？
いいえ
ステップ455
ステップ458
継続して使用
はい
インストールされた制御プログラムが消滅
ステップ456
通常の電子計算機と同様の使い方
ステップ457
エンド

[図13]


スタート
ＵＳＢコネクターを切断
ステップ450
アンインストールを開始？
ステップ451
いいえ
はい
制御プログラムを無効？
ステップ470
はい
いいえ
使用したユーザデータを削除？
ステップ476
いいえ
はい
制御プログラムを削除？
ステップ471
いいえ
はい
ステップ458
継続して使用
ステップ477
電子計算機内のユーザデータを削除
使用したユーザデータを削除？
ステップ472
いいえ
はい
ステップ478
制御プログラムを無効
電子計算機内のデータを削除
ステップ473
インストールされた制御プログラムが消滅
ステップ474
通常の電子計算機と同様の使い方
ステップ475
エンド

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/011783

A. CLASSIFICATION OF SUBJECT MATTER
Int.Cl[7] G06F12/14, G06F1/00, G06F3/06

According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
Int.Cl[7] G06F12/14, G06F1/00, G06F3/06

Documentation searched other than minimum documentation to the extent that such documents are included in the fields searched
Jitsuyo Shinan Koho 1922-1996 Jitsuyo Shinan Toroku Koho 1996-2004
Kokai Jitsuyo Shinan Koho 1971-2004 Toroku Jitsuyo Shinan Koho 1994-2004

Electronic data base consulted during the international search (name of data base and, where practicable, search terms used)

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2002-041442 A (Sony Computer Entertainment Inc.), 08 February, 2002 (08.02.02), All pages; all drawings & US 2002/0016908 A1 & WO 2002/010906 A2	1-21
Y	WO 2001/061692 A1 (TREK 2000 INTERNATIONAL LTD.), 23 August, 2001 (23.08.01), All pages; all drawings & US 2002/0010827 A1 & US 2002/0174287 A1	1-21

☒ Further documents are listed in the continuation of Box C. ☐ See patent family annex.

* Special categories of cited documents:
"A" document defining the general state of the art which is not considered to be of particular relevance
"E" earlier application or patent but published on or after the international filing date
"L" document which may throw doubts on priority claim(s) or which is cited to establish the publication date of another citation or other special reason (as specified)
"O" document referring to an oral disclosure, use, exhibition or other means
"P" document published prior to the international filing date but later than the priority date claimed
"T" later document published after the international filing date or priority date and not in conflict with the application but cited to understand the principle or theory underlying the invention
"X" document of particular relevance; the claimed invention cannot be considered novel or cannot be considered to involve an inventive step when the document is taken alone
"Y" document of particular relevance; the claimed invention cannot be considered to involve an inventive step when the document is combined with one or more other such documents, such combination being obvious to a person skilled in the art
"&" document member of the same patent family

Date of the actual completion of the international search	Date of mailing of the international search report
14 October, 2004 (14.10.04)	02 November, 2004 (02.11.04)
Name and mailing address of the ISA/ Japanese Patent Office	Authorized officer
Facsimile No.	Telephone No.

Form PCT/ISA/210 (second sheet) (January 2004)

INTERNATIONAL SEARCH REPORT

International application No.
PCT/JP2004/011783

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevant to claim No.
Y	JP 2001-229017 A (Besu Tekunoroji Kabushiki Kaisha), 24 August, 2001 (24.08.01), All pages; all drawings & US 2001/0014883 A1 & EP 1126357 A3	1-21

国際調査報告

国際出願番号　PCT／JP2004／011783

A.　発明の属する分野の分類（国際特許分類（IPC））
Int.Cl.[7]　G06F12/14, G06F1/00, G06F3/06

B.　調査を行った分野
調査を行った最小限資料（国際特許分類（IPC））
Int.Cl.[7]　G06F12/14, G06F1/00, G06F3/06

最小限資料以外の資料で調査を行った分野に含まれるもの
日本国実用新案公報　1922－1996年
日本国公開実用新案公報　1971－2004年
日本国実用新案登録公報　1996－2004年
日本国登録実用新案公報　1994－2004年

国際調査で使用した電子データベース（データベースの名称、調査に使用した用語）

C.　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 2002-041442 A（株式会社ソニー・コンピュータエンタテインメント）2002.02.08, 全頁, 全図 & US 2002/0016908 A1 & WO 2002/010906 A2	1-21
Y	WO 2001/061692 A1（トレック・2000・インターナショナル・リミテッド）2001.08.23, 全頁, 全図 & US 2002/0010827 A1 & US 2002/0174287 A1	1-21

☒ C欄の続きにも文献が列挙されている。　☐ パテントファミリーに関する別紙を参照。

＊ 引用文献のカテゴリー
「A」特に関連のある文献ではなく、一般的技術水準を示すもの
「E」国際出願日前の出願または特許であるが、国際出願日以後に公表されたもの
「L」優先権主張に疑義を提起する文献又は他の文献の発行日若しくは他の特別な理由を確立するために引用する文献（理由を付す）
「O」口頭による開示、使用、展示等に言及する文献
「P」国際出願日前で、かつ優先権の主張の基礎となる出願の日の後に公表された文献
「T」国際出願日又は優先日後に公表された文献であって出願と矛盾するものではなく、発明の原理又は理論の理解のために引用するもの
「X」特に関連のある文献であって、当該文献のみで発明の新規性又は進歩性がないと考えられるもの
「Y」特に関連のある文献であって、当該文献と他の１以上の文献との、当業者にとって自明である組合せによって進歩性がないと考えられるもの
「&」同一パテントファミリー文献

国際調査を完了した日	国際調査報告の発送日
14.10.2004	02.11.2004

国際調査機関の名称及びあて先
日本国特許庁（ISA／JP）
郵便番号１００－８９１５
東京都千代田区霞が関三丁目４番３号

特許庁審査官（権限のある職員）　5N　3044
髙橋　克

電話番号　０３－３５８１－１１０１　内線　３５８５

国際調査報告

国際出願番号　ＰＣＴ／ＪＰ２００４／０１１７８３

C（続き）．　関連すると認められる文献

引用文献のカテゴリー＊	引用文献名　及び一部の箇所が関連するときは、その関連する箇所の表示	関連する請求の範囲の番号
Y	JP 2001-229017 A (ベーステクノロジー株式会社) 2001.08.24, 全頁, 全図 & US 2001/0014883 A1 & EP 1126357 A3	1-21